RECEIVED
CENTRAL FAX CENTER
JUL 05 2006

ZILKA·KOTAB
PC
ZILKA, KOTAB & FEECE™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	July 5, 2006	**Phone Number**	**Fax Number**
To:	Board of Patent Appeals		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAI1P484/01.103.01 **App. No: 10/028,906**

Total Number of Pages Being Transmitted, Including Cover Sheet: 30

Message:

Please deliver to the Board of Patent Appeals.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

PAGE 1/30 * RCVD AT 7/5/2006 6:38:16 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/33 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):05-52

RECEIVED
CENTRAL FAX CENTER

JUL 05 2006

Practitioner's Docket No. NAI1P484/01.103.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Nicholas Paul Kelly et al.

Application No.: 10/028,906 Group No.: 2131
Filed: 12/28/2001 Examiner: Laforgia, C.
For: CONTROLLING ACCESS TO SUSPICIOUS FILES

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. Transmitted herewith, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on March 20, 2006, and the Notice of Panel Decision from Pre-Appeal Brief Review mailed June 5, 2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

(When using Express Mail, the Express Mail label number is mandatory; Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

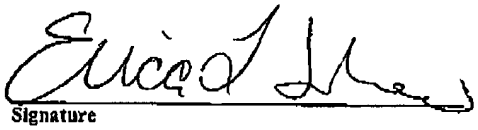
37 C.F.R. § 1.8(a)
_with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_as "Express Mail Post Office to Addressee"
Mailing Label No. _____ (mandatory)

TRANSMISSION

facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

Date: 7/5/2006



Signature

Erica L. Farlow

(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

RECEIVED
CENTRAL FAX CENTER

JUL 05 2006

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$500.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $500.00 to Deposit Account No. 50-1351 (Order No. NAI1P484).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P484).

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

RECEIVED
CENTRAL FAX CENTER
JUL 05 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Kelly et al.	Group Art Unit: 2131
Application No. 10/028,906	Examiner: LAFORGIA, CHRISTIAN A.
Filed: 12/28/2001	Date: 07/05/2006
For: CONTROLLING ACCESS TO SUSPICIOUS FILES	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on 03/20/2006, and the Notice of Panel Decision from Pre-Appeal Brief Review mailed June 05, 2006.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER
VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-39

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-39
3. Claims allowed: None
4. Claims rejected: 1-39
5. Claims cancelled: None

C. CLAIMS ON APPEAL

The claims on appeal are: 1-39

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to Claims 1, 14, and 27; a computer program product, method, and data processing apparatus for operating a computer, as seen in Figures 1-7, are provided to review files for potential malware. In use, logging code is operable to maintain a statistical log having an entry for each file sent to the computer for review. See page 10, lines 13-15, for example. Each entry is arranged to store a count value indicating the number of times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file. See page 10, lines 15-17, for example. In addition, weighting table code is operable to maintain a weighting table (e.g. Figure 7) identifying, for each value of said one or more predetermined attributes, a weighting indicating the likelihood that a file having that value of said one or more predetermined attributes will be malware. See page 10, lines 17-20, for example. Further, statistical log interface code is operable, upon receipt of a file, to determine with reference to the statistical log the count value relating to that file. See page 10, lines 20-22, for example. Also, action determination code is operable, if the count value determined by the statistical log interface code exceeds a predetermined threshold, to reference the weighting table to determine the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with that file in the statistical log. See page 10, lines 22-26, for example. Moreover, action performing code is operable to perform predetermined actions in relation to the file dependent on the weighting determined by said action determination code. See page 10, lines 26-28, for example.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-13 under 35 U.S.C. 101 as being directed toward non-statutory subject matter.

Issue # 2: The Examiner has rejected Claims 1-2, 7-12, 14-15, 20-25, 27-28, and 33-38 under 35 U.S.C. 103(a) as being unpatentable over Chess et al. (U.S. Patent No. 6,711,583), in view of Smithson et al. (U.S. Patent No. 6,886,099).

Issue # 3: The Examiner has rejected Claims 3-6, 13, 16-19, 26, 29-32, and 39 under 35 U.S.C. 103(a) as being unpatentable over Chess in view of Smithson in view of Templeton (U.S. Patent No. 6,401,210).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1-13 under 35 U.S.C. 101 as being directed toward non-statutory subject matter.

Group #1: Claims 1-13

The Examiner has rejected Claims 1-13 under 35 U.S.C. 101 as being non-statutory, since such claims allegedly represent a computer listing *per se*, that is, non-functional descriptive material, etc. Appellant respectfully disagrees. Specifically, appellant clearly claims a "computer program product for operating a computer to review files for potential malware" (emphasis added), clearly a functional set of acts being performed.

Issue # 2:

The Examiner has rejected Claims 1-2, 7-12, 14-15, 20-25, 27-28, and 33-38 under 35 U.S.C. 103(a) as being unpatentable over Chess et al. (U.S. Patent No. 6,711,583), in view of Smithson et al. (U.S. Patent No. 6,886,099).

Group #1: Claims 1-2, 7-10, 12, 14-15, 20-23, 25, 27-28, and 33-36, 38

With respect to each of the independent claims, the Examiner has responded to appellant's arguments with respect to appellant's claimed "logging code operable to maintain a statistical log having an entry for each file sent to the computer for review, each entry being arranged to store a count value indicating the number of times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file" (see this or similar, but not necessarily identical language in each of the independent claims).

Specifically, the Examiner has stated that the Abstract of Smithson teaches "the tracking for a number of times a file is sent for review." Appellant respectfully asserts that the Abstract in Smithson only discloses measuring "how many E-mail messages are sent having an identical file attachment, the file type or simply in total." Clearly, measuring how many E-mail messages are sent, as in Smithson, does not meet appellant's specific claim language, namely "stor[ing] a count value indicating the number of times that the file has been sent to the computer for review" (emphasis added), as claimed.

In addition, the Examiner has stated that Col. 5, lines 5-48 in Chess teach "keeping a value of one or more predetermined attributes relating to the file, such as whether the file is safe or questionable." First, appellant respectfully asserts that such excerpt in Chess only teaches "examin[ing] documents in the collection on disk," and not "a statistical log having an entry for each file sent to the computer for review," as appellant claims (emphasis added). Second, Chess merely discloses storing "the document name and macro data" associated with the document, where the macro data is the names of any macro data stored in the document. Clearly, such data does not meet appellant's claimed "value of one or more predetermined attributes relating the file" (emphasis added). Thus, in view of the above arguments, appellant respectfully asserts that neither Smithson nor Chess meet appellant's specific claim language.

Still with respect to each of the independent claims, the Examiner has responded to appellant's claimed "weighting indicating the likelihood that a file having that value of said one or more predetermined attributes will be malware" and "referenc[ing] the weighting table to determine the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with that file in the statistical log" (see this or similar, but not necessarily identical language in each of the independent claims).

Specifically, the Examiner has argued that "Chess discloses a technique for determining the likelihood of a file being infected by the addition or change of code since the last time the file has been reviewed" (Col. 5, lines 5-48). Appellant respectfully asserts that simply comparing macro data to determine if "safe" changes or "questionable" changes have occurred, as in Chess, does not even suggest any sort of weighting table. Instead, Chess teaches that "removing one or

more macros from the document could be considered 'safe', whereas the modification or addition of macros to the document could be considered 'questionable'."

Thus, Chess determines whether a document has safe or questionable changes made to it based on whether a change involved the removal or addition of macros, which clearly does not even suggest the utilization of a weighting table, and especially not in the context claimed by appellant. In addition, since Chess does not disclose storing any sort of value of one or more predetermined attributes relating to the file, in the manner claimed by appellant, Chess simply would not utilize a weighting table for determining the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with that file, as appellant specifically claims.

Still with respect to each of the independent claims, the Examiner has failed to responded to appellant's arguments with respect to appellant's claimed "statistical log interface code operable, upon receipt of a file, to determine with reference to the statistical log the count value relating to that file; action determination code operable, if the count value determined by the statistical log interface code exceeds a predetermined threshold" (see this or similar, but not necessarily identical language in each of the independent claims). In particular, the Examiner has merely stated that "the combination of [Smithson and Chess] disclose referencing a weighting table to determine the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with that file in the statistical log."

Appellant respectfully asserts that what is claimed is "determin[ing] with reference to the statistical log the count value relating to that file" (emphasis added). For substantially the reasons argued above, appellant emphasizes that neither Chess nor Smithson teach any sort of value in the context claimed by appellant, and thus it is impossible for the references to teach a situation where "upon receipt of a file...determin[ing] with reference to the statistical log the count value relating to that file," as claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine

reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, at least for the reasons noted above. Thus, a notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group #2: Claims 11, 24, and 37

Appellant further notes that the Examiner has failed to respond to appellant's arguments with respect to dependent Claim 11 et al. Appellant again notes that the Examiner has relied on the following excerpts from the Smithson reference to make a prior art showing of appellant's claimed "each entry in the statistical log ... further arranged to identify, for each sender of that file, the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent" (see this or similar, but not necessarily identical language in each of the independent claims).

> "As preferred examples of the measurement parameters that may be used there are proposed:
> 1. How many E-mail messages are sent having an identical message title.
> 2. How many E-mail messages are sent identical file attachment.
> 3. How many email messages are sent having a file attachment of a given file type.
> 4. How many E-mail messages are sent having a file attachment that is an executable file.
> 5. The E-mail through put within the computer system.
> 6. The E-mail throughput measured in a form dependent upon a number of E-mails multiplied by a total size for the E-mails." (Col. 4, lines 25-40)

Again, as noted above, Smithson's measurement parameters and thresholds are associated with aggregate file activity, and not a particular file. To this end, Smithson simply fails to meet appellant's claimed "number of times that that sender has sent the file in addition to the count

value indicating the total number of times that the file has been sent." It is further noted that the measurement parameters does not track a per-sender number, and thus fails to meet appellant's claimed "each entry in the statistical log ... further arranged to identify, for each sender of that file, the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent" (emphasis added).

Thus, only appellant teaches and claims use of both 1) a number of times that a particular sender has sent a file, and 2) a total number of times the file has been sent *irrespective of sender* in each entry in the statistical log. Note Table 1 below which illustrates such claimed subject matter.

Table 1

Entry_1 (associated with file_1)

Sender_1

Number of times file_1 is sent by Sender_1

Sender_2

Number of times file_1 is sent by Sender_2

Total number of times file_1 is sent

Entry_2 (associated with file_2)

Sender_1

Number of times file_2 is sent by Sender_1

Sender_2

Number of times file_2 is sent by Sender_2

Total number of times file_2 is sent

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 3:

The Examiner has rejected Claims 3-6, 13, 16-19, 26, 29-32, and 39 under 35 U.S.C. 103(a) as being unpatentable over Chess in view of Smithson in view of Templeton (U.S. Patent No. 6,401,210).

Group #1: Claims 3-6, 13, 16-19, 26, 29-32, and 39

Appellant respectfully asserts that such claims are not met by the prior art for at least the reasons argued with respect to Issue #2, Group #1.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Original) A computer program product for operating a computer to review files for potential malware, comprising:

logging code operable to maintain a statistical log having an entry for each file sent to the computer for review, each entry being arranged to store a count value indicating the number of times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file;

weighting table code operable to maintain a weighting table identifying, for each value of said one or more predetermined attributes, a weighting indicating the likelihood that a file having that value of said one or more predetermined attributes will be malware;

statistical log interface code operable, upon receipt of a file, to determine with reference to the statistical log the count value relating to that file;

action determination code operable, if the count value determined by the statistical log interface code exceeds a predetermined threshold, to reference the weighting table to determine the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with that file in the statistical log; and

action performing code operable to perform predetermined actions in relation to the file dependent on the weighting determined by said action determination code.

2. (Original) A computer program product as claimed in claim 1, wherein said one or more predetermined attributes comprise an indication of the file type of the file.

3. (Original) A computer program product as claimed in claim 1, wherein if the weighting indicates that the file is probably malware, said action performing code is operable to perform the steps of:

(i) encrypting the file such that only an administrator can decrypt that file; and

(ii) generating for access by an administrator a notification identifying that the file has been encrypted.

4. (Original) A computer program product as claimed in claim 3, wherein the action performing code is further operable to associate a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted.

5. (Original) A computer program product as claimed in claim 1, wherein if the weighting indicates that the file is possibly malware, said action performing code is operable to perform the steps of:

(i) encrypting the file such that only an administrator or the originator of the file can decrypt that file; and

(ii) generating for access by an administrator a notification identifying that the file has been encrypted.

6. (Original) A computer program product as claimed in claim 5, wherein the action performing code is further operable to associate a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted.

7. (Original) A computer program product as claimed in claim 1, wherein if the weighting indicates that the file is to be treated with caution, said action performing code is operable to perform the steps of:

(i) associating a warning message with the file for reference by a person receiving that file; and

(ii) generating for access by an administrator a notification identifying the file.

8. (Original) A computer program product as claimed in claim 1, wherein if the weighting indicates that the file is safe, said action performing code is operable to generate for access by an administrator a notification identifying the file.

9. (Original) A computer program product as claimed in claim 1, wherein if it is determined that a file sent to the computer is not currently entered in the statistical log, the logging code is further operable to create an entry in the statistical log for the file, in which the value of said one or more predetermined attributes relating to the file are stored, and in which the count value is

initialised.

10. (Original) A computer program product as claimed in claim 1, wherein upon receipt of a file, the statistical log interface code is operable to cause the count value within the relevant entry of the statistical log to be incremented to account for the current occurrence of the file.

11. (Original) A computer program product as claimed in claim 1, wherein the computer is arranged to review files included in e-mail communications, and each entry in the statistical log is further arranged to identify, for each sender of that file, the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent.

12. (Original) A computer program product as claimed in claim 11, wherein upon receipt of a file, the statistical log interface code is operable to cause the count value within the relevant entry of the statistical log to be incremented to account for the current occurrence of the file, and the number by which the count value is incremented is dependent on the number of times that the sender of the current occurrence of the file has previously sent that file.

13. (Original) A computer program product as claimed in claim 1, wherein if said action performing code is arranged, dependent on the weighting, to encrypt the file, the computer program product further comprises:

automated decryption code operable, if the file is subsequently determined to be safe, to perform the steps of:

(i) locating all encrypted occurrences of that file on a file system; and

(ii) decrypting each said occurrence.

14. (Original) A method of operating a computer to review files for potential malware, comprising the steps of:

(a) maintaining a statistical log having an entry for each file sent to the computer for review, each entry being arranged to store a count value indicating the number of times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file;

(b) maintaining a weighting table identifying, for each value of said one or more predetermined attributes, a weighting indicating the likelihood that a file having that value of said one or more predetermined attributes will be malware;

(c) upon receipt of a file, determining with reference to the statistical log the count value relating to that file;

(d) if the count value determined at said step (c) exceeds a predetermined threshold, referencing the weighting table to determine the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with that file in the statistical log; and

(e) performing predetermined actions in relation to the file dependent on the weighting determined at said step (d).

15. (Original) A method as claimed in claim 14, wherein said one or more predetermined attributes comprise an indication of the file type of the file.

16. (Original) A method as claimed in claim 14, wherein if the weighting indicates that the file is probably malware, said step (e) comprises the steps of:

(i) encrypting the file such that only an administrator can decrypt that file; and

(ii) generating for access by an administrator a notification identifying that the file has been encrypted.

17. (Original) A method as claimed in claim 16, further comprising the step of associating a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted.

18. (Original) A method as claimed in claim 14, wherein if the weighting indicates that the file is possibly malware, said step (e) comprises the steps of:

(i) encrypting the file such that only an administrator or the originator of the file can decrypt that file; and

(ii) generating for access by an administrator a notification identifying that the file has been encrypted.

19. (Original) A method as claimed in claim 18, further comprising the step of associating a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted.

20. (Original) A method as claimed in claim 14, wherein if the weighting indicates that the file is to be treated with caution, said step (e) comprises the steps of:

(i) associating a warning message with the file for reference by a person receiving that file; and

(ii) generating for access by an administrator a notification identifying the file.

21. (Original) A method as claimed in claim 14, wherein if the weighting indicates that the file is safe, said step (e) comprises the step of generating for access by an administrator a notification identifying the file.

22. (Original) A method as claimed in claim 14, wherein if at said step (c) it is determined that the file is not currently entered in the statistical log, the method further comprises the step of creating an entry in the statistical log for the file, in which the value of said one or more predetermined attributes relating to the file are stored, and in which the count value is initialised.

23. (Original) A method as claimed in claim 14, wherein said step (c) includes the step of incrementing within the statistical log the count value to account for the current occurrence of the file.

24. (Original) A method as claimed in claim 14, wherein the computer is arranged to review files included in e-mail communications, and each entry in the statistical log is further arranged to identify, for each sender of that file, the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent.

25. (Original) A method as claimed in claim 24, wherein said step (c) includes the step of incrementing within the statistical log the count value to account for the current occurrence of the file, and the number by which the count value is incremented is dependent on the number of times that the sender of the current occurrence of the file has previously sent that file.

26. (Original) A method as claimed in claim 14, wherein if at said step (e), the file is encrypted, the method further comprises, if the file is subsequently determined to be safe, the automated steps of:

locating all encrypted occurrences of that file on a file system; and

decrypting each said occurrence.

27. (Original) A data processing apparatus for reviewing files for potential malware, comprising:

logging logic operable to maintain a statistical log having an entry for each file sent to the computer for review, each entry being arranged to store a count value indicating the number of times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file;

weighting table logic operable to maintain a weighting table identifying, for each value of said one or more predetermined attributes, a weighting indicating the likelihood that a file having that value of said one or more predetermined attributes will be malware;

statistical log interface logic operable, upon receipt of a file, to determine with reference to the statistical log the count value relating to that file;

action determination logic operable, if the count value determined by the statistical log interface logic exceeds a predetermined threshold, to reference the weighting table to determine the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with that file in the statistical log; and

action performing logic operable to perform predetermined actions in relation to the file dependent on the weighting determined by said action determination logic.

28. (Original) A data processing apparatus as claimed in claim 27, wherein said one or more predetermined attributes comprise an indication of the file type of the file.

29. (Original) A data processing apparatus as claimed in claim 27, wherein if the weighting indicates that the file is probably malware, said action performing logic is operable to perform the steps of:

(i) encrypting the file such that only an administrator can decrypt that file; and

(ii) generating for access by an administrator a notification identifying that the file has been encrypted.

30. (Original) A data processing apparatus as claimed in claim 29, wherein the action performing logic is further operable to associate a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted.

31. (Original) A data processing apparatus as claimed in claim 27, wherein if the weighting indicates that the file is possibly malware, said action performing logic is operable to perform the steps of:

(i) encrypting the file such that only an administrator or the originator of the file can decrypt that file; and

(ii) generating for access by an administrator a notification identifying that the file has been encrypted.

32. (Original) A data processing apparatus as claimed in claim 31, wherein the action performing logic is further operable to associate a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted.

33. (Original) A data processing apparatus as claimed in claim 27, wherein if the weighting indicates that the file is to be treated with caution, said action performing logic is operable to perform the steps of:

(i) associating a warning message with the file for reference by a person receiving that file; and

(ii) generating for access by an administrator a notification identifying the file.

34. (Original) A data processing apparatus as claimed in claim 27, wherein if the weighting indicates that the file is safe, said action performing logic is operable to generate for access by an administrator a notification identifying the file.

35. (Original) A data processing apparatus as claimed in claim 27, wherein if it is determined that a file sent to the computer is not currently entered in the statistical log, the logging logic is

further operable to create an entry in the statistical log for the file, in which the value of said one or more predetermined attributes relating to the file are stored, and in which the count value is initialised.

36. (Original) A data processing apparatus as claimed in claim 27, wherein upon receipt of a file, the statistical log interface logic is operable to cause the count value within the relevant entry of the statistical log to be incremented to account for the current occurrence of the file.

37. (Original) A data processing apparatus as claimed in claim 27, wherein the computer is arranged to review files included in e-mail communications, and each entry in the statistical log is further arranged to identify, for each sender of that file, the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent.

38. (Original) A data processing apparatus as claimed in claim 37, wherein upon receipt of a file, the statistical log interface logic is operable to cause the count value within the relevant entry of the statistical log to be incremented to account for the current occurrence of the file, and the number by which the count value is incremented is dependent on the number of times that the sender of the current occurrence of the file has previously sent that file.

39. (Original) A data processing apparatus as claimed in claim 27, wherein if said action performing logic is arranged, dependent on the weighting, to encrypt the file, the data processing apparatus further comprises:

automated decryption logic operable, if the file is subsequently determined to be safe, to perform the steps of:

(i) locating all encrypted occurrences of that file on a file system; and

(ii) decrypting each said occurrence.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

There is no such related proceeding.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P484/01.103.01).

Respectfully submitted,

By: _____ Date: 7/5/06

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660